Hantera datorn

Business Desktops

Dokumentets artikelnummer: 312947-102

September 2003

Denna handbok innehåller definitioner och instruktioner för säkerhetsfunktioner och Intelligent Manageability som finns förinstallerade i vissa modeller.

VARNING! Den här texten ger information om att allvarliga personskador eller dödsfall kan uppstå om instruktionerna inte följs.

SE UPP! Den här texten innehåller varningar om att utrustningen kan förstöras eller information förloras om inte instruktionerna följs.

Hantera datorn
Business Desktops

Andra upplagan (September 2003)
Dokumentets artikelnummer: 312947-102

Innehåll

Hantera datorn

Index

Hantera datorn

HP Intelligent Manageability ger standardbaserade lösningar för hantering och kontroll av stationära och bärbara datorer samt arbetsstationer i nätverksmiljö. HP introducerade år 1995 branschens första system för fullständig styrbarhet av datorer. HP har patenterat tekniken för denna styrbarhet. Sedan dess har HP lett branschens gemensamma strävan efter nödvändig standard och infrastruktur för att effektivt kunna installera, konfigurera och styra stationära och bärbara datorer samt arbetsstationer. HP samarbetar intimt med ledande tillverkare av styrprogramvara för att garantera en kompatibilitet mellan Intelligent Manageability och dessa produkter. Intelligent Manageability är en viktig aspekt av vårt omfattande åtagande att förse dig med lösningar som är till hjälp i de fyra faserna av en dators livscykel – planering, installation, hantering och övergångar.

Huvudfunktionerna och fördelarna i datorhanteringen är:

- Första konfigurering och installation
- Fjärrinstallation
- Uppdatering och hantering av program
- ROM-uppdatering
- Inventariekontroll och säkerhet/skydd
- Felmeddelanden och återställning

Stödet för de olika funktionerna som beskrivs i handboken kan variera med modell och programversion.

Första konfigurering och installation

Datorn levereras med en förinstallerad systemprogramprofil. Efter en snabb "programuppackning" kan du börja använda datorn.

Du vill kanske byta ut den förinstallerade programprofilen mot en anpassad profil med system- och användarprogram. Det finns flera olika sätt att installera en egen programprofil. Dessa är:

- Installera extra program efter det att den förinstallerade programprofilen har "packats upp".
- Använda verktyg för programinstallation, såsom Altiris Deployment Solution™, för att byta ut den förinstallerade programprofilen mot en anpassad.
- Använda en diskkloningsprocess för att kopiera innehållet från en hårddisk till en annan.

Den bästa installationsmetoden beror på befintliga tekniska resurser och processer. Avsnittet PC Deployment (Ställa iordning PC:n) på HPs webbplats Lifecycle Solutions (http://h18000.www1.hp.com/solutions/pcsolutions) innehåller information som kan hjälpa dig att välja den bästa installationsmetoden.

Cd-skivan *Restore Plus!,* ROM-baserad installation och ACPI-maskinvara ger ytterligare hjälp att återställa systemprogramvara, konfigurering, felsökning och strömsparfunktioner.

Fjärrinstallation

Med fjärrinstallationsfunktionen (Remote System Installation) kan du starta och ställa in datorn med hjälp av program- och konfigurationsinformationen som finns i en nätverksserver genom att starta PXE (Preboot Execution Environment). Fjärrinstallationsfunktionen används oftast som ett verktyg för inställning och konfiguration av systemet och kan användas till följande uppgifter:

- Formatera en hårddisk
- Installera en programprofil på en eller flera nya persondatorer
- Fjärruppdatering av systemets BIOS i flash-ROM ("Fjärruppgradering av ROM" på sidan 7)
- Konfigurering av systemets BIOS-inställningar

För att starta fjärrinstallationen trycker du på **F12** när meddelandet F12 = Network Service Boot visas i nedre högra hörnet i fönstret med HPs logotyp. Följ instruktionerna på skärmen för att fortsätta. Standardstartordningen är en BIOS-konfigurationsinställning som kan ändras så att den alltid försöker starta från PXE.

HP och Altiris, Inc. samarbetar för att utveckla verktyg för enklare hantering och installation av företagens datorer, vilket ska sänker totalkostnaderna och göra HP-datorerna till företagets mest hanterbara klientdatorer.

Uppdatering och hantering av programvara

HP tillhandahåller flera verktyg för hantering och uppdatering av programvara i stationära datorer och arbetsstationer – Altiris; Altiris PC Transplant Pro; HP Client Manager Software (en Altiris-lösning); System Software Manager; Proactive Change Notification; och ActiveUpdate.

HP Client Manager Software (HPs CMS)

HPs CMS (HP Client Manager Software) integrerar intimt tekniken från HP Intelligent Manageability i Altiris för att erbjuda överlägsen maskinvarukontroll för HP-enheterna, bland annat:

- Detaljerade bilder av maskinvaran för inventariekontroll
- Övervakning och diagnostik av datorernas "hälso"-status
- Meddelanden i förväg om ändringar av maskinvaran
- Rapportering av viktig information på webben, såsom maskiner med varningsmeddelanden om överhettning, minnesvarningar m.m.
- Fjärruppdatering av systemprogramvara såsom drivrutiner och ROM BIOS
- Fjärrändring av startordning

Mer information om HP Client Manager finns på http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Solutions

HP Client Management Solutions erbjuder centraliserad maskinvaruhantering för HP-klientenheter för alla områden inom den informationsteknologiska livscykeln.

- Inventariehantering
  - ❏ Licenskompabilitet som gäller Sverige
  - ❏ PC-kontroll och rapportering
  - ❏ Hyreskontrakt, åtgärda inventariekontroll
- Installation och migrering/överflyttning
  - ❏ Microsoft Windows 2000-, Windows XP Professional- eller Home Edition-migrering
  - ❏ Installation av datorn
  - ❏ Typmigreringar

- Teknisk hjälp och problemlösning
  - Hantering av hjälpetiketter
  - Fellösning från fjärransluten dator
  - Problemlösning med hjälp av fjärransluten dator
  - Återställa operativsystem, programvaruinställningar och datafiler på hårddisken åt kund
- Hantering och användning av programvara
  - Pågående datorhantering
  - HP-system SW-installation
  - Självhjälp för program

På vissa bordsdator- och notebook-modeller finns ett Altiris-hanteringsprogram med i den fabriksladdade profilen. Med detta kan du kommunicera med Altiris Development Solution för att utföra installationen av ny maskinvara eller typmigrering till ett nytt operativsystem med hjälp av enkla anvisningar. Altiris-lösningarna erbjuder enkla funktioner för programvarudistribution. Tillsammans med SSM (System Software Manager) eller HP Client Manager kan administratörerna dessutom uppdatera ROM BIOS och enhetens drivrutiner från en central manöverpanel.

Mer information finns på adressen http://www.hp.com/go/easydeploy.

Altiris PC Transplant Pro

Altiris PC Transplant Pro gör PC-migreringen enkel genom att gamla inställningar, alternativ och data bibehålls och flyttas över till den nya miljön snabbt och enkelt. Uppgraderingar tar någon minut i stället för timmar eller dagar, och datorns skrivbord ser ut och fungerar precis som användarna är vana vid.

Mer information och anvisningar om hur du laddar ner en fullt funktionsduglig 30-dagars utvärderingsversion finns på adressen http://h18000.www1.hp.com/im/prodinfo.html#deploy.

System Software Manager

Med SSM (System Software Manager) kan du uppdatera systemprogram på flera datorer samtidigt. Vid körning i ett klientbaserat system upptäcker SSM både maskin- och programvaruversioner och uppdaterar sedan rätt program från ett centralt lagringsutrymme, en filmapp. Drivrutinversioner som stöds av SSM är märkta med en särskild ikon på webbplatsen där dessa kan hämtas. De finns också på cd-skivan Support Software. Du kan hämta programmet eller få information om SSM på http://h18000.www1.hp.com/im/ssmwp.html.

Product Change Notification (Meddelande om ändring av produkt)

PCN-programmet använder Subscriber's Choice-webbplatsen för att proaktivt och automatiskt:

- Skicka PCN-meddelanden (Product Change Notification) till dig via e-post, för att informera dig om ändringar av maskin- och programvara för flertalet kommersiella datorer och servrar, upp till 60 dagar i förväg.
- Skicka e-post med Kund-, Råd-, Upplysnings- och Säkerhetsmeddelanden samt drivrutinvarningar till dig för flertalet kommersiella datorer och servrar.

Du kan anpassa din egen profil, så att du bara erhåller den typ av information som är viktig för en speciell IT-miljö. Mer information om Proactive Change Notification-programmet och om hur du skapar en anpassad profil finns på adressen http://www.hp.com/go/pcn.

ActiveUpdate

ActiveUpdate är ett klientbaserat program från HP. ActiveUpdate-klienten körs i den lokala datorn och använder de användardefinierade inställningarna för att proaktivt och automatiskt hämta programuppdateringar för flertalet kommersiella HP-datorer och -servrar. Dessa nedladdade programuppdateringar kan installeras i de maskiner för vilka de är avsedda av HP Client Manager Software och System Software Manager.

För att lära dig mer om ActiveUpdate, hur du laddar ner programmet och anpassar det, hänvisas till: http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html.

ROM-flash

Datorn levereras med ett programmerbart flash-ROM (read only memory). Genom att skapa ett setup-lösenord i setup-programmet (F10) kan du skydda ROM från att oavsiktligt uppdateras eller skrivas över. Detta är viktigt för att garantera datorns driftsäkerhet. Om du behöver eller vill uppgradera ROM kan du:

- Beställa en uppgraderad ROMPaq-diskett från HP.
- Ladda ned de senaste ROMPaq-bilderna från http://h18000.www1.hp.com/im/ssmwp.html.

SE UPP! För maximalt ROM-skydd måste du skapa ett setup-lösenord. Setup-lösenordet skyddar mot obehöriga uppgraderingar av ROM. Med SSM (System Software Manager) kan systemadministratören ange setup- lösenordet i en eller flera datorer samtidigt. Mer information finns på http://h18000.www1.hp.com/im/ssmwp.html.

Fjärruppgradering av ROM

Med hjälp av fjärruppgradering av ROM kan systemadministratören göra en säker uppgradering av ROM av fjärr-HP-datorer direkt från en central plats i nätverket. Genom att systemadministratören kan fjärruppgradera flera datorer och persondatorer centralt, erhåller man en enhetlig installation och större kontroll över ROM-profilerna i nätverkets HP-datorer. Det ökar också produktiviteten och ger lägre totalkostnad för datorerna.

Datorn måste vara på eller startas med Remote Wakeup för att du ska kunna dra fördel av fjärruppgraderingen av ROM.

Mer information om fjärruppgradering av ROM finns i HP Client Manager Software eller System Software Manager på adressen http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

HPQFlash-programmet används för att lokalt uppdatera eller återställa system-ROM på enskilda datorer via ett Windows-operativsystem.

Mer information om HPQFlash finns på adressen http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html.

Felsäkert ROM-startblock

Ett felsäkert ROM-startblock gör att systemet kan återställas om ROM-uppgraderingen mot förmodan misslyckas, t ex om ett strömavbrott inträffar under själva uppgraderingen. Startblocket är en flash-skyddad sektion av ROM som kontrollerar att ett giltigt system-ROM finns varje gång systemet startas.

- Om system-ROM är giltigt startar systemet normalt.
- Om systemets ROM inte klarar validitetskontrollen, ger det felsäkra startblocket i ROM tillräckligt stöd för att starta systemet från en ROMPaq-diskett, som programmerar systemets ROM med en giltig profil.

Om startblocket känner av ett ogiltigt system-ROM, blinkar på/av-lampan RÖTT 8 gånger med en sekunds mellanrum och därefter med två sekunders uppehåll. Samtidigt hörs 8 ljudsignaler. Ett meddelande visas på skärmen om återställningläge för startblock (vissa modeller).

För att återställa systemet från detta läge gör du på följande sätt:

1. Om det finns en diskett i diskettenheten, tar du ut den och stänger sedan av datorn.
2. Sätt in en ROMPaq-diskett i diskettenheten.
3. Starta datorn.
4. Om systemet inte hittar någon ROMPaq-diskett, får du ett meddelande om att sätta in en sådan och starta om datorn.
5. Om ett setup-lösenord har skapats, börjar Caps Lock-lampan att lysa och du uppmanas att ange lösenordet.
6. Ange setup-lösenordet.

7. Om det sker en lyckad start från disketten och ROM-minnet omprogrammeras, börjar de tre lamporna på tangentbordet att lysa. En serie stigande ljudsignaler signalerar också att uppgraderingen lyckades.
8. Ta ut disketten och stäng av datorn.
9. Starta om datorn.

I följande tabell visas de olika kombinationerna av lampsignaler på tangentbordet som startblocks-ROM använder (när ett PS/2-tangentbord är anslutet till datorn). Dessutom visas förklaringar och åtgärder för de olika kombinationerna.

Kombinationer av tangentbordslampor som används av startblocks-ROM

Felsäkert startblocks-läge	Tangent-bordslam-pornas färg	Tangentbords-lampornas signal	Betydelse/Meddelande
Num Lock	Grön	Lyser	ROMPaq diskett saknas, är trasig eller diskettenheten är ej klar.
Caps Lock	Grön	Lyser	Ange lösenord.
Num, Caps, Scroll Lock	Grön	Lampblink på i följd, en åt gången–N, C, SL	Tangentbordet låst i nätverksläge.
Num, Caps, Scroll Lock	Grön	Lyser	Uppgradering av startblock i ROM lyckades. Stäng av datorn och starta sedan om den.

✎ Diagnostiska lampor blinkar inte på USB-tangentbord.

Kopiera konfigureringen

Med de här procedurerna kan administratören enkelt kopiera en konfiguration till andra datorer av samma modell. Det ger en snabbare, mer enhetlig konfiguration av flera datorer.

Båda procedurerna kräver en diskettenhet eller en USB-flashmediaenhet med stöd, till exempel en HP Drive Key.

Kopiering till en enstaka dator

SE UPP! En setup-konfigurering är modellspecifik. Filsystemet kan skadas om käll- och måldator inte är av samma modell. Kopiera till exempel inte setup-konfigureringen från en D510 Ultra-slim Desktop (hypertunn skrivbordsmodell) till en D510 e-dator.

1. Välj en setup-konfigurering som du önskar kopiera. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start > Avsluta > Starta om datorn**.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. Sätt i en diskett eller en USB-flashmediaenhet.
4. Klicka på **Arkiv Spara på diskett**. Följ instruktionerna på skärmen för att skapa konfigureringsdisketten eller USB-flashmediaenheten.
5. Stäng av datorn som ska konfigureras och sätt i konfigureringsdisketten eller USB-flashmediaenheten.
6. Starta datorn som ska konfigureras. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.
7. Klicka på **Arkiv Återställ från diskett** och följ instruktionerna på skärmen.
8. Starta om datorn när konfigureringen är slutförd.

Kopiera till flera datorer

SE UPP! En setup-konfigurering är modellspecifik. Filsystemet kan skadas om käll- och måldator inte är av samma modell. Kopiera till exempel inte setup-konfigureringen från en D510 Ultra-slim Desktop (hypertunn skrivbordsmodell) till en D510 e-dator.

Med den här metoden tar det lite längre tid att förbereda konfigureringsdisketten eller USB-flashmediaenheten, men det går avsevärt mycket snabbare att kopiera konfigureringen till måldatorerna.

En startdiskett kan inte skapas i Windows 2000. Det behövs en startdiskett för den här proceduren eller för att skapa en startbar USB-flashmediaenhet. Om Windows 9x eller Windows XP inte är tillgängliga för att skapa en startdiskett, kan du använda metoden för kopiering till en enstaka dator i stället (se "Kopiering till en enstaka dator" på sidan 10).

1. Skapa en startdiskett eller en USB-flashmediaenhet. Se "Startdiskett" på sidan 12, "Stödd USB-flashmediaenhet" på sidan 13, eller "USB-flashmediaenhet utan stöd" på sidan 16.

SE UPP! Alla datorer kan inte startas från en USB-flashmediaenhet. Om den standardmässiga startordningen i setup-programmet (F10) anger USB-enheten före hårddisken, kan datorn startas från en USB-flashmediaenhet. I annat fall måste en startdiskett användas.

2. Välj en setup-konfigurering som du önskar kopiera. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start > Avsluta > Starta om datorn**.
3. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

4. Sätt i en startdiskett eller en USB-flashmediaenhet.
5. Klicka på **Arkiv > Spara på diskett**. Följ instruktionerna på skärmen för att skapa konfigureringsdisketten eller USB-flashmediaenheten.
6. Ladda ned ett BIOS-program för kopiering av konfigureringen (repset.exe) och kopiera det på konfigureringsdisketten eller USB-flashmediaenheten. Programmet kan du hitta på adressen http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html.
7. Skapa en autoexec.bat-fil på konfigureringsdisketten eller USB-flashmediaenheten som innehåller följande kommando:

   repset.exe
8. Stäng av datorn som ska konfigureras. Sätt i konfigureringsdisketten eller USB-flashmediaenheten och starta datorn. Konfigureringsprogrammet körs automatiskt.
9. Starta om datorn när konfigureringen är slutförd.

Skapa en startenhet

Startdiskett

De här instruktionerna är avsedda för Windows XP Professional och Home Edition. I Windows 2000 finns inget stöd för att skapa startdisketter.

1. Sätt i en diskett i diskettenheten.
2. Klicka på **Start** och klicka sedan på **Den här datorn**.
3. Högerklicka på enhetsbokstaven och välj därefter **Formatera**.
4. Markera kryssrutan **Skapa en MS-DOS-startdiskett** och klicka sedan på **Start**.

Gå tillbaka till "Kopiera till flera datorer" på sidan 11.

Stödd USB-flashmediaenhet

Enheter som stöds, såsom en HP Drive Key eller en DiskOnKey, har en förinställd profil för att förenkla processen att göra dem startbara. Om den Drive Key som används saknar den här bilden, använd då proceduren senare i det här avsnittet (se "USB-flashmediaenhet utan stöd" på sidan 16).

SE UPP! Alla datorer kan inte startas från en USB-flashmediaenhet. Om den standardmässiga startordningen i setup-programmet (F10) anger USB-enheten före hårddisken, kan datorn startas från en USB-flashmediaenhet. I annat fall måste en startdiskett användas.

För att skapa en startbar USB-flashmediaenhet måste du ha:

- Ett av följande system:
  - Compaq Evo D510 Ultra-slim Desktop
  - Compaq Evo D510 Convertible Minitower (omvandlingsbart minitorn)/Small Form Factor (liten formfaktor)
  - HP Compaq Business Desktop d530 Series – Ultra-slim Desktop, Small Form Factor eller Convertible Minitower
  - Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c eller N1000c Notebooks
  - Compaq Presario 1500 eller 2800 Notebooks

  Beroende på individuella BIOS kan kommande system ge stöd åt start för HP Drive Key.

SE UPP! Om du använder en annan dator än en av de som nämns ovan, bör du förvissa dig om att den standardmässiga startordningen i konfigureringsprogrammet anger USB-enheten före hårddisken.

- En av följande lagringsmoduler:
  - 16 MB HP Drive Key
  - 32 MB HP Drive Key
  - 32 MB DiskOnKey
  - 64 MB HP Drive Key
  - 64 MB DiskOnKey
  - 128 MB HP Drive Key
  - 128 MB DiskOnKey

- En startbar DOS-diskett med FDISK- och SYS-programmen. Om inte SYS är tillgängligt kan FORMAT användas, men alla befintliga filer på Drive Key förloras.

1. Stäng av datorn.
2. Sätt i Drive Key i en av datorns USB-portar och ta bort alla andra USB-lagringsenheter utom USB-diskettenheterna.
3. Sätt i en startbar DOS-diskett med FDISK.COM och antingen SYS.COM eller FORMAT.COM i en diskettenhet och sätt på datorn så att den startar upp från DOS-disketten.
4. Kör FDISK från A:\ prompt genom att skriva **FDISK** och trycka på Retur. När du blir tillfrågad svara då **Ja** (**J**) för att aktivera stort diskstöd.
5. Ange Choice (Urval) [**5**] för att visa enheterna i systemet. Drive Key blir den enhet som storleksmässigt passar bäst bland enheterna i listan. Oftast är det den sista enheten i listan. Anteckna enhetsbokstaven.

   Drive Key-enhet: _____

SE UPP! Fortsätt inte, om en enhet inte passar Drive Key. Dataförluster kan uppstå. Kontrollera om det finns ytterligare lagringsenheter i någon av USB-portarna. Om det finns någon, ta då bort dessa, starta om datorn och fortsätt från steg 4. Om det inte finns någon, då stöder antingen systemet inte Drive Key eller så är Drive Key felaktig. FORTSÄTT INTE att försöka göra Drive Key startbar.

6. Avsluta FDISK genom att trycka på **Esc** för att gå tillbaka till A:\ prompt.
7. Gå till steg 8, om den startbara DOS-disketten innehåller SYS.COM. Gå i annat fall till steg 9.
8. Vid A:\ prompt skriver du **SYS x:** där x representerar enhetsbokstaven ovan. Gå till steg 13.

SE UPP! Kontrollera att du har skrivit korrekt enhetsbokstav för Drive Key.

När systemfilerna har överförts återgår SYS till A:\ prompt.

9. Kopiera alla filer som du vill bevara från Drive Key i en temporär mapp i en annan enhet (till exempel i systemets hårddisk).
10. Vid A:\ prompt skriver du **FORMAT /S X:** där X representerar enhetsbokstaven som nämndes ovan.

SE UPP! Kontrollera att du har skrivit korrekt enhetsbokstav för Drive Key.

FORMAT visar ett eller flera varningsmeddelanden och varje gång tillfrågas du, om du vill fortsätta. Svara **j** varje gång. FORMAT formaterar Drive Key, lägger till systemfilerna och ber dig ange en volymetikett.

11. Tryck på **Retur** om du inte vill ange etikett eller ange, om du så önskar, en etikett.
12. Kopiera tillbaka eventuella filer som du sparade i steg 9 till Drive Key.
13. Ta ur disketten och starta om datorn. Datorn startar nu upp från Drive Key som enhet C.

Den standardmässiga startordningen varierar från dator till dator och kan ändras i setup-programmet (F10).

Om du har använt en DOS-version från Windows 9x, visas Windows-logon en kort stund. Om du inte vill att den här bilden ska visas, lägg då till en fil med längden noll och namnet LOGO.SYS i rotkatalog för Drive Key.

Gå tillbaka till "Kopiera till flera datorer" på sidan 11.

USB-flashmediaenhet utan stöd

SE UPP! Alla datorer kan inte startas från en USB-flashmediaenhet. Om den standardmässiga startordningen i setup-programmet (F10) anger USB-enheten före hårddisken, kan datorn startas från en USB-flashmediaenhet. I annat fall måste en startdiskett användas.

För att skapa en startbar USB-flashmediaenhet måste du ha:

- Ett av följande system:
  - Compaq Evo D510 Ultra-slim Desktop
  - Compaq Evo D510 Convertible Minitower (omvandlingsbart minitorn)/Small Form Factor (liten formfaktor)
  - HP Compaq Business Desktop d530 Series – Ultra-slim Desktop, Small Form Factor eller Convertible Minitower
  - Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c eller N1000c Notebooks
  - Compaq Presario 1500 eller 2800 Notebooks

  Beroende på det individuella BIOS kan kommande system även ge stöd åt start för en USB-flashmediaenhet.

SE UPP! Om du använder en annan dator än en av de som nämns ovan, bör du förvissa dig om att den standardmässiga startordningen i konfigureringsprogrammet anger USB-enheten före hårddisken.

- En startbar DOS-diskett med FDISK- och SYS-program. Om inte SYS är tillgängligt kan FORMAT användas, men alla befintliga filer på Drive Key förloras.

1. Om det finns något PCI-kort i systemet med anslutna SCSI-, ATA RAID- eller SATA-enheter, stäng då av datorn och dra ut nätsladden.

SE UPP! Nätsladden FÅR inte vara ansluten.

2. Öppna datorn och ta bort PCI-korten.
3. Sätt i USB-flashmediaenheten i en av datorns USB-portar och ta bort alla övriga USB-lagringsenheter utom USB-diskettenheterna. Sätt tillbaka datorluckan.

4. Sätt i nätsladden och starta datorn. Så fort den gröna lampan på skärmen lyser, trycker du på **F10**-tangenten för att öppna setup-programmet.
5. Gå till Avancerat/PCI-enheter för att avaktivera både IDE- och SATA-styrenheterna. När du avaktiverar SATA-styrenheten, bör du anteckna vilken IRQ som styrenheten är tilldelad. Du måste tilldela om IRQ:n senare. Avsluta setup, och bekräfta ändringarna.

   SATA IRQ: _____
6. Sätt i en startbar DOS-diskett med FDISK.COM och antingen SYS.COM eller FORMAT.COM i en diskettenhet och sätt på datorn så att den startar upp från DOS-disketten.
7. Kör FDISK och radera alla eventuella partitioner på USB-flashmediaenheten. Skapa en ny partition och makera den som aktiv. Avsluta FDISK genom att trycka på **Esc**.
8. Om inte systemet startar om automatiskt när du avslutar FDISK, trycker du på **Ctrl+Alt+Del** för att starta om med DOS-disketten.
9. Vid A:\-prompten skriver du **FORMAT C: /S** och trycker på **Retur**. Format-kommandot formaterar USB-flashmediaenheten, lägger till systemfilerna och ber dig ange en volymetikett.
10. Tryck på **Retur** om du inte vill ange etikett eller ange, om du så önskar, en etikett.
11. Stäng av datorn och dra ut nätsladden. Öppna datorn och installera om eventuella PCI-kort som du tog bort tidigare. Sätt tillbaka datorluckan.
12. Sätt i nätsladden, ta ur disketten och starta datorn.
13. Så fort den gröna lampan på skärmen lyser, trycker du på **F10**-tangenten för att öppna setup-programmet.
14. Gå till Avancerat/PCI-enheter och aktivera IDE- och SATA-styrenheterna som du avaktiverade i steg 5 på nytt. Ange den ursprungliga IRQ:n för SATA-styrenheten.

15. Spara ändringarna och avsluta. Datorn startar nu upp från USB-flashmediaenheten som enhet C.

Den standardmässiga startordningen varierar från dator till dator och kan ändras i setup-programmet (F10).

Om du har använt en DOS-version från Windows 9x, visas Windows-logon en kort stund. Om du inte vill att den här bilden ska visas, lägg då till en fil med längden noll och med namnet LOGO.SYS i rotkatalog för Drive Key.

Gå tillbaka till "Kopiera till flera datorer" på sidan 11.

På/Av-knapp med två lägen

Med ACPI (Advanced Configuration and Power Interface) aktiv i Windows 2000 och Windows XP Professionell samt Home Edition kan på/av-knappen ställas in så att den antingen fungerar som en strömbrytare eller som en vilolägesknapp. Vilolägesfuktionen stänger inte av datorn helt utan är ett standby-läge med lägre strömförbrukning. Det gör att du snabbt kan stänga av utan att avsluta program och lika snabbt återgå till samma läge utan förlust av data.

Konfigurera om på/av-knappen så här:

1. I Windows 2000 vänsterklickar du på **Start** och väljer sedan **Inställningar > Kontrollpanel > Energialternativ**.

   I Windows XP Professional och Home Edition vänsterklickar du på **Start** och väljer **Kontrollpanel > Prestanda och underhåll > Energialternativ**.

2. I **Egenskaper för enegialternativ** väljer du fliken **Avancerat**.
3. Under **På/Av-knapp** väljer du önskad knappinställning.

När du har konfigurerat på/av-knappen som en vilolägesknapp, använder du den för att få systemet i ett läge med låg strömförbrukning (vänteläge). När du trycker på knappen igen, återgår systemet till normalläge. Om du vill stänga av strömmen till systemet helt, håller du knappen intryckt i fyra sekunder.

SE UPP! Använd inte på/av-knappen för att stänga av datorn såvida inte systemet har hängt sig. Avstängning med på/av-knappen utan att operativsystemet först stängs kan skada eller förstöra data på hårddisken.

Webbplats

HP utför noggranna tester och felsöker program som utvecklats av HP och tredjepartsleverantörer, och utvecklar dessutom hjälpprogram som integreras med operativsystemet för att ge högsta möjliga prestanda, kompatibilitet och tillförlitlighet för HP-datorerna.

Vid övergången till ett nytt eller uppdaterat operativsystem är det viktigt att installera hjälpprogram som är utvecklade för just detta operativsystem. Om du tänker köra en version av Microsoft Windows som skiljer sig från den version som levererades med datorn, måste du installera motsvarande drivrutiner och hjälpprogram så att alla funktioner stöds och fungerar som de ska.

HP har gjort det enklare att hitta, komma åt, utvärdera och installera de senaste hjälpprogrammen. Du kan hämta programvaran från http://www.hp.com/support.

Webbplatsen innehåller de senaste drivrutinerna, hjälpprogrammen och ROM-profilerna som behövs för att köra de senaste versionerna av Microsoft Windows operativsystem i din HP-dator.

Byggblock och partners

HPs hanteringslösningar integreras med andra systemhanteringsprogram och är baserade på industristandarderna såsom:

- Desktop Management Interface (DMI) 2.0
- WOL-tekniken (Wake on LAN)
- ACPI
- SMBIOS
- Stöd för PXE (Pre-boot Execution)

Inventariekontroll och säkerhet

Funktionerna för inventariekontroll som är inbyggda i datorn ger användaren möjlighet att samla in inventariedata, som kan hanteras av HP Insight Manager, HP Client Manager eller andra systemhanteringsprogram. Eftersom inventariefunktionerna automatiskt och intimt integreras med dessa hanteringsverktyg, kan du använda det verktyg som passar bäst i ditt system och få ut det mesta möjliga av de verktyg som du redan har.

HP erbjuder också flera lösningar för att kontrollera åtkomsten till viktiga komponenter och information. ProtectTools Embedded Security (Inbyggd skyddsanordning), om sådan finns, förhindrar obehörig åtkomst till data och kontrollerar systemets integritet samt kontrollerar den uppgivna identiteten hos tredjepart-användare som försöker använda datorn. Skyddsfunktioner såsom ProtectTools, Smart Cover Sensor och Smart Cover Lock finns på vissa modeller och hindrar obehöriga från att öppna datorn och komma åt dess inre komponenter. Du kan skydda värdefulla datatillgångar genom att avaktivera parallell-, seriella och USB-portar eller genom att avaktivera start från flyttbara enheter. Larm från Memory Change och Smart Cover Sensor kan skickas automatiskt till systemhanteringsprogram, som ger en tidig varning om att någon försöker mixtra med datorns inre komponenter.

ProtectTools, Smart Cover Sensor och Smart Cover Lock finns som tillval i vissa system.

Använd följande program för att hantera skyddsinställningarna i din HP-dator:

- Lokalt, med hjälp av funktionerna i setup-programmet. Mer information om setup-programmet och hur det används finns i *Konfigureringshandboken* som medföljde datorn.
- Fjärrhantering med HP Client Manager eller System Software Manager. Dessa program möjliggör en säker och enhetlig uppgradering och kontroll av skyddsinställningar från ett enkelt kommandoradsprogram.

Följande tabell och avsnitt visar lokal hantering av säkerhetsfunktioner i datorn med setup-programmet.

Säkerhetsfunktioner, översikt

Funktion	Syfte	Aktivering av funktionen
Styrning av start från flyttbart medium	Hindrar start från flyttbart medium. (finns på vissa enheter)	Från setup-programmets meny.
Styrning av Seriellt, Parallellt, USB eller infrarött gränssnitt	Hindrar överföring av data via det inbyggda seriella, parallella, USB (universal serial bus) eller infraröda gränssnittet.	Från setup-programmets meny.
Power-On Password (Start-lösenord)	Hindrar användning av datorn tills ett lösenord har angivits. Det kan gälla både start och omstart av systemet.	Från setup-programmets meny.
Lösenord för Setup-programmet	Hindrar att datorn konfigureras om (användning av setup-programmet) tills lösenordet har angivits.	Från setup-programmets (F10) meny.
Inbyggd säkerhetsanordning	Förhindrar obehörig åtkomst till data med hjälp av kryptering och lösenordsskydd. Kontrollerar systemets integritet och kontrollerar identiteten hos tredjepart-användare som försöker använda datorn.	Från setup-programmets (F10) meny.
DriveLock	Hindrar obehörig åtkomst till data på MultiBay-hårddiskar. Denna funktion finns bara på vissa modeller.	Från setup-programmets (F10) meny.

✎ Mer information om setup-programmet finns i *Konfigureringshandboken*.
Stöd för säkerhetsfunktioner kan variera beroende på datorkonfigurationen.

Säkerhetsfunktioner, översikt *(Fortsättning)*

Funktion	Syfte	Aktivering av funktionen
SmartCover-sensor	Indikerar att datorns lock eller sidoplåt har tagits bort. Kan ställas in så att lösenord krävs vid omstart av datorn när locket eller sidoplåten har tagits bort. Mer information om denna funktion finns i *Referenshandboken* på cd-skivan *Documentation Library*. Denna funktion finns bara på vissa modeller.	Från setup-programmets (F10) meny.
Master Boot Record Security (MBR-säkerhet)	Kan hindra oavsiktliga eller uppsåtliga ändringar av MBR på aktuell startdisk och ger möjlighet att återställa till senaste kända, fungerande MBR.	Från setup-programmets (F10) meny.
Meddelande vid minnesändring	Upptäcker när minnesmoduler har lagts till, flyttats eller tagits bort och varnar användaren och systemadministratören.	Mer information om Meddelande vid minnesändring finns i online-handboken *Intelligent Manageability- handboken*.

✎ Mer information om setup-programmet finns i *Konfigureringshandboken*.
Stöd för säkerhetsfunktioner kan variera beroende på datorkonfigurationen.

Säkerhetsfunktioner, översikt *(Fortsättning)*

Funktion	Syfte	Aktivering av funktionen
Ägarmärkning	Visar information om innehavaren, som den angetts av systemadministratören, under uppstart (skyddas av setup-lösenordet).	Från setup-programmets (F10) meny.
Kabellåsfäste	Förhindrar åtkomst till datorns inre för att förhindra oönskade ändringar av konfiguration eller att komponenter avlägsnas. Kan också användas för att låsa fast datorn så att den inte kan stjälas.	Installera ett kabellås så att datorn är låst vid något fast föremål.
Säkerhetskabel	Förhindrar åtkomst till datorns inre för att förhindra oönskade ändringar av konfiguration eller att komponenter avlägsnas.	Installera ett lås i säkerhets-kabeln för att för4hindra oönskade ändringar av konfigurationen eller att komponenter avlägsnas.

✎ Mer information om setup-programmet finns i *Konfigureringshandboken*.
Stöd för säkerhetsfunktioner kan variera beroende på datorkonfigurationen.

Lösenordsskydd

Startlösenordet hindrar obehörig användning av datorn, då det måste anges för att komma åt program eller data i datorn varje gång datorn startas eller startas om. Setup-lösenordet förhindrar särskilt obehörig åtkomst till setup-programmet och kan också användas för att komma förbi startlösenordet. När du uppmanas att ange startlösenordet, kan du i stället ange setup-lösenordet för att kunna använda datorn.

En nätverksinstallation av setup-lösenordet kan skapas så att systemadministratören kan logga in i alla system i nätverket och underhålla dem utan att känna till startlösenordet, även om ett sådant har ställts in.

Ställa in ett setup-lösenord med setup-programmet

Om systemet är utrustat med en inbyggd säkerhetsanordning hänvisas till "Embedded Security (Inbyggd säkerhet)" på sidan 29.

Om du ställer in ett setup-lösenord med setup-programmet kan inte datorn konfigureras om (med setup-programmet) förrän lösenordet har angivits.

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start >Avsluta > Starta om datorn**.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. Välj **Säkerhet,** sedan **Setup-lösenord** och följ instruktionerna på skärmen.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna** och **Avsluta**.

Att ställa in ett startlösenord med hjälp av setup-programmet

Om du ställer in ett startlösenord med setup-programmet förhindras åtkomst till datorn, om du inte först anger lösenordet när du startar datorn. Om ett startlösenord ställts in, visas Password Options (Lösenordsalternativ) i setup-programmet på Säkerhetsmenyn. Bland lösenordsalternativen finns också lösenord vid omstart. Om Password Prompt on Warm Boot (Lösenord vid omstart) är på, måste lösenordet också anges varje gång datorn startas om.

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start >Avsluta > Starta om datorn**.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. Välj **Säkerhet,** sedan **Power-On Password (Startlösenord)** och följ instruktionerna på skärmen.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna** och **Avsluta**.

Ange ett startlösenord

Så här anger du ett startlösenord:

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start >Avsluta > Starta om datorn**.
2. När nyckelikonen visas på skärmen, anger du aktuellt lösenord och trycker sedan på **Retur**.

Skriv noga; av säkerhetsskäl visas inte tecknen som du skriver på skärmen.

Om du anger ett felaktigt lösenord, visas en ikon som föreställer en avbruten nyckel. Försök på nytt. Efter tre misslyckade försök måste du stänga av datorn och sedan starta om den innan du kan fortsätta.

Ange ett setup-lösenord

Om systemet är utrustat med en inbyggd säkerhetsanordning hänvisas till "Embedded Security (Inbyggd säkerhet)" på sidan 29.

Om ett setup-lösenord har ställts in för datorn måste detta anges varje gång du kör setup-programmet.

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start >Avsluta > Starta om datorn**.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. När nyckelikonen visas på skärmen skriver du lösenordet och trycker på **Retur**.

Skriv noga; av säkerhetsskäl visas inte tecknen som du skriver på skärmen.

Om du anger ett felaktigt lösenord, visas en ikon som föreställer en avbruten nyckel. Försök på nytt. Efter tre misslyckade försök måste du stänga av datorn och sedan starta om den innan du kan fortsätta.

Ändra ett start- eller setup-lösenord

Om systemet är utrustat med en inbyggd säkerhetsanordning hänvisas till "Embedded Security (Inbyggd säkerhet)" på sidan 29.

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start >Avsluta > Starta om datorn**. Om du vill ändra setup-lösenordet startar du **setup-programmet**.
2. När nyckelikonen visas, anger du aktuellt lösenord, ett snedstreck (/) eller en annan teckenavgränsare, det nya lösenordet, ett till snedstreck (/) eller en annan teckenavgränsare och det nya lösenordet igen enligt nedan:
   aktuellt lösenord/nytt lösenord/nytt lösenord

Skriv noga; av säkerhetsskäl visas inte tecknen som du skriver på skärmen.

3. Tryck på **Retur**.

Det nya lösenordet gäller nästa gång du startar datorn.

Mer information om andra teckenavgränsare finns på "Avgränsare för landsspecifikt tangentbord" på sidan 28. Start- och setup-lösenordet kan också ändras från Security options (Säkerhetsalternativ) i setup-programmet.

Ta bort ett start- eller setup-lösenord

Om systemet är utrustat med en inbyggd säkerhetsanordning hänvisas till "Embedded Security (Inbyggd säkerhet)" på sidan 29.

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start >Avsluta > Starta om datorn**. Om du vill ta bort setup-lösenordet startar du **setup-programmet**.
2. När nyckelikonen visas, skriver du det aktuella lösenordet följt av ett snedstrck (/) eller en annan teckenavgränsare: **aktuellt lösenord/**
3. Tryck på **Retur**.

Mer information om andra teckenavgränsare finns på "Avgränsare för landsspecifikt tangentbord". Start- och setup-lösenordet kan också ändras från Security options (Säkerhetsalternativ) i setup-programmet.

Avgränsare för landsspecifikt tangentbord

Alla tangentbord har utformats för att uppfylla landsspecifika krav. Syntax och tecken som används för att ändra eller ta bort lösenord beror på vilket tangentbord, som levererades med datorn.

Avgränsare för landsspecifikt tangentbord

Arabiskt	/	Grekiskt	-	Ryskt	/
Belgiskt	=	Hebreiskt	.	Slovakiskt	-
BHKSJ*	-	Ungerskt	-	Spanskt	-
Brasilianskt	/	Italienskt	-	Svenskt/Finskt	/
Kinesiskt	/	Japanskt	/	Schweiziskt	-
Tjeckiskt	-	Koreanskt	/	Taiwanesiskt	/
Danskt	-	Latinamerikanskt	-	Thailändskt	/
Franskt	!	Norskt	-	Turkiskt	.
Fransk-kanadensiskt	é	Polskt	-	Brittisk-engelskt	/
Tyskt	-	Portugisiskt	-	Amerikansk-engelskt	/

* För Bosnien-Herzegovina, Kroatien, Slovenien och Jugoslavien

Radera lösenord

Om du glömmer lösenordet får du inte tillgång till datorn. Instruktioner för att ta bort lösenord finns i *Felsökningshandboken*.

Om systemet är utrustat med en inbyggd säkerhetsanordning hänvisas till "Embedded Security (Inbyggd säkerhet)."

Embedded Security (Inbyggd säkerhet)

ProtectTools inbyggda säkerhetsanordning kombinerar kryptering med lösenordsskydd för att ge ett bättre skydd för fil/katalog-kryptering av Embedded File System (EFS) och säker e-posthantering vid användning av Microsoft Outlook och Outlook Express. ProtectTools finns tillgängligt för vissa "business desktops" som Configured-To-Order (CTO)-tillval. Det är avsett för HP-kunder där datasäkerheten är av största betydelse: obehörig åtkomst till data utgör en mycket större fara än förlust av data. ProtectTools använder fyra lösenord:

- (F10) Setup – för att komma åt setup-programmet (F10) och aktivera/avaktivera ProtectTools
- Take ownership [Ta äganderätt] – anges och används av en systemadministratör, som ger behörighet åt användare och ställer in säkerhetsparametrar
- Emergency recovery Token [Nödåterställningstecken (för behörighet)] – anges av systemadministratören och möjliggör återställning i händelse av funktionsavbrott för dator- eller ProtectTools-chip
- Basic User (Huvudanvändare) – anges och används av slutanvändaren.

Om slutanvändarens har tappat/glömt bort sitt lösenord, kan krypterad data inte återställas. ProtectTools används säkrast när data i användarens enhet kopieras till en dators informationsystem eller att säkerhetskopior görs regelbundet.

ProtectTools Embedded Security [Inbyggd säkerhetsanordning] är ett TCPA 1.1-kompatibelt säkerhetschip som har installerats som tillval på vissa 'business desktops'-moderkort. Varje ProtectTools Embedded Security-chip är unikt och bundet till en viss dator. Varje chip utför speciella säkerhetsprocesser oberoende av övriga datorkomponenter (exempelvis processor, minne eller operativsystem).

En dator med aktiverat ProtectTools Embedded Security kompletterar och förstärker de redan inbyggda säkerhetsfunktionerna i Microsoft Windows 2000, Windows XP Professional eller Home Edition. Medan till exempel operativsystemet kan kryptera lokala filer och mappar baserat på en EFS, bildar ProtectTools Embedded Security ytterligare ett skyddslager genom att skapa kryptonycklar från systemets rootnyckel (som finns lagrad i kisel). Den här processen kallas "inpackning" av kryptonycklarna. ProtectTools förhindrar inte nätverksåtkomst till en dator som saknar ProtectTools.

Huvudfunktionerna hos ProtectTools Embedded Security inkluderar:

- Systemautenticering
- Skyddad lagring
- Dataintegritet

SE UPP! Skydda lösenorden. **Krypterad data är inte åtkomlig och kan inte heller återskapas utan lösenorden**.

Ställa in lösenord

Setup (Inställningar)

Ett setup-lösenord kan skapas och den inbyggda säkerhetsanordningen kan aktiveras med setup-programmet F10.

1. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

2. Använd upp- eller ned-piltangenterna för att välja språk och tryck därefter på **Retur**.
3. Använd vänster eller höger piltangent för att gå till fliken **Säkerhet**. Använd sedan upp- eller ned-pilen för att gå till **Setup-lösenord**. Tryck på **Retur**.

4. Skriv ett lösenord och bekräfta det. Tryck på **F10** för att godkänna lösenordet.

Skriv noga; av säkerhetsskäl visas inte tecknen som du skriver på skärmen.

5. Använd upp- eller ned-piltangenterna för att gå till **Embedded Security Device [Inbyggd säkerhetsanordning]**. Tryck på **Retur**.
6. Om alternativet **Embedded Security Device – Disable [Inbyggd säkerhetsanordning – Avaktivera]** är markerat i dialogrutan, använder du vänster eller höger piltangent för att ändra markeringen till **Embedded Security Device – Enable [Inbyggd säkerhetsanordning – Aktivera]**. Tryck på **F10** för att godkänna den ändrade markeringen.

SE UPP! Om du markerar **Reset to Factory Settings – Reset [Återställ fabriksinställningarna – Återställ]** raderas alla nycklar och den krypterade datan kan inte återställas, *om du inte* har säkerhetskopierat nycklarna (se "Take Ownership (Ta äganderätt) och Emergency Recovery Token (Nödåterställningstecken)"). Markera bara **Återställ** när du ombeds göra detta, när du ska återställa krypterad data (se "Återskapa krypterade data" på sidan 34).

7. Använd vänster eller höger piltangent för att gå till **Arkiv**. Använd upp- eller ned-piltangenterna för att gå till **Save Changes and Exit [Spara ändringarna och Avsluta]**. Tryck på **Retur**, och därefter på **F10** för att bekräfta.

Take Ownership (Ta äganderätt) och Emergency Recovery Token (Nödåterställningstecken)

Lösenordet för Take Ownership krävs för att aktivera eller avaktivera säkerhetssystemet och för att kunna ge användarbehörighet. Nödåterställningsmekanismen gör att användare kan erhålla behörighet och data bli åtkomligt, om den inbyggda säkerhetsanordningen inte svarar.

1. Om du använder Windows XP Professional eller Home Edition klickar du på **Start > All Programs [Starta alla program] > HP ProtectTools Inbyggda säkerhetsverktyg > Initieringsguide för den inbyggda säkerhetsanordningen**.

   Om du använder Windows 2000 klickar du på **Start > Programs [Starta program] > HP ProtectTools inbyggda säkerhetsverktyg > Initieringsguide för den inbyggda säkerhetsanordningen**.

2. Klicka på **Nästa**.
3. Skriv ett Take Ownership-lösenord, bekräfta detta och klicka sedan på **Nästa**.

Skriv noga; av säkerhetsskäl visas inte tecknen som du skriver på skärmen.

4. Klicka på **Nästa** för att godkänna standardplatsen för Återställningsarkivet.
5. Skriv ett Emergency Recovery-lösenord, bekräfta detta och klicka sedan på **Nästa**.
6. Sätt i en diskett som du kan spara Nyckeln till Nödåterställningstecken på. Klicka på **Bläddra** och markera disketten.

SE UPP! Nyckeln till Nödåterställningstecken används för att återskapa krypterad data vid ett eventuellt datorhaveri eller om det inbyggda säkerhetschipset inte svarar. **Data kan inte återställas utan nyckeln**. (Åtkomst till data är inte heller möjlig utan Basic User-lösenordet.) Förvara den här disketten på en säker plats.

7. Klicka på **Spara** för att godkänna platsen och standardfilnamnet och klicka sedan på **Nästa**.
8. Klicka på **Nästa** för att bekräfta inställningarna innan säkerhetssystemet har initierats.

Ett meddelande visas eventuellt om att de inbyggda säkerhetsfunktionerna inte har initierats. Klicka inte i meddelandet; detta ska användas senare i proceduren och meddelandet försvinner efter någon sekund.

9. Klicka på **Nästa** för att komma förbi konfigurering av lokala bestämmelser.

10. Kontrollera att kryssrutan för Start av initieringsguide för den inbyggda säkerhetsanordningen [Start Embedded Security User Initialization Wizard] är markerad och klicka sedan på **Avsluta**.

Användarinitieringsguiden startar nu automatiskt.

Basic User

Under initieringen skapas Basic User-lösenordet. Detta lösenord krävs för att kunna skriva och komma åt krypterad data.

SE UPP! Skydda Basic User-lösenordet. **Krypterad data är inte åtkomlig och kan inte heller återställas utan detta lösenord**.

1. Gör så här om inte Användarinitieringsguiden är öppen:

   Om du använder Windows XP Professional eller Home Edition klickar du på **Start > All Programs [Starta alla program] > HP ProtectTools inbyggda säkerhetsverktyg > Användarinitieringsguiden**.

   Om du använder Windows 2000 klickar du på **Start > Programs [Starta program] > HP ProtectTools inbyggda säkerhetsverktyg > Användarinitieringsguiden**.

2. Klicka på **Nästa**.
3. Skriv ett Basic User-lösenord, bekräfta detta och klicka sedan på **Nästa**.

Skriv noga; av säkerhetsskäl visas inte tecknen som du skriver på skärmen.

4. Klicka på **Nästa** för att godkänna inställningarna.
5. Välj lämpliga säkerhetsfunktioner och klicka på **Nästa**.
6. Markera lämplig e-postklient genom att klicka på den och därefter på **Nästa**.
7. Klicka på **Nästa** för att tillämpa Encryption Certificate [Kryptocertifikat].
8. Klicka på **Nästa** för att godkänna inställningarna.
9. Klicka på **Slutför**.
10. Starta om datorn.

Återskapa krypterade data

För att återställa data efter utbyte av ProtectTools-chipset måste du ha följande:

- SPEmRecToken.xml – Nyckeln till Nödåterställningstecken
- SPEmRecArchive.xml – dold mapp, standardplats: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- ProtectTools-lösenord
  - ❏ Inställningar
  - ❏ Take Ownership
  - ❏ Emergency Recovery Token
  - ❏ Basic User

1. Starta om datorn.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. Skriv Setup-lösenordet och tryck sedan på **Retur**.
4. Använd upp- eller ned-piltangenterna för att välja språk och tryck därefter på **Retur**.
5. Använd vänster eller höger piltangent för att gå till fliken **Säkerhet**. Använd sedan upp- eller ned-pilen för att gå till **Inbyggd säkerhetsanordning**. Tryck på **Retur**.
6. Gör så här om endast ett alternativ, **Embedded Security Device – Disable (inbyggd säkerhetsanordning – avaktivera)**, är tillgängligt:
   a. Använd vänster eller höger piltangent för att ändra det till **Embedded Security Device [Inbyggd säkerhetsanordning] Enable (Aktivera)**. Tryck på **F10** för att godkänna den ändrade markeringen.

b. Använd vänster eller höger piltangent för att gå till **Arkiv**. Använd upp- eller ned-piltangenterna för att gå till **Save Changes and Exit [Spara ändringarna och Avsluta]**. Tryck på **Retur**, och därefter på **F10** för att bekräfta.

c. Gå till steg 1.

Om två alternativ är tillgängliga går du till steg 7.

7. Använd upp- eller nedpiltangenten för att gå till **Reset to Factory Settings – Do Not Reset [Återställ fabriksinställningarna – Återställ inte]**. Tryck på vänster eller höger piltangent en gång.

   Följande meddelande visas på skärmen: Om du utför den här åtgärden återställs den inbyggda säkerhetsanordningen till fabriksinställning, om inställningarna sparas före avslutning. Tryck på valfri tangent för att fortsätta.

   Tryck på **Retur**.

8. Alternativet lyder nu **Reset to Factory Settings – Reset [Återställ fabriksinställningarna – Återställ]**. Tryck på **F10** för att godkänna den ändrade markeringen.

9. Använd vänster eller höger piltangent för att gå till **Arkiv**. Använd upp- eller ned-piltangenterna för att gå till **Save Changes and Exit [Spara ändringarna och Avsluta]**. Tryck på **Retur**, och därefter på **F10** för att bekräfta.

10. Starta om datorn.

11. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

---

12. Skriv Setup-lösenordet och tryck sedan på **Retur**.

13. Använd upp- eller ned-piltangenterna för att välja språk och tryck därefter på **Retur**.

14. Använd vänster eller höger piltangent för att gå till fliken **Säkerhet**. Använd sedan upp- eller ned-pilen för att gå till **Inbyggd säkerhetsanordning**. Tryck på **Retur**.

15. Om alternativet **Embedded Security Device – Disable [Inbyggd säkerhetsanordning – Avaktivera]** är markerat i dialogrutan, använder du vänster eller höger piltangent för att ändra markeringen till **Embedded Security Device – Enable [Inbyggd säkerhetsanordning – Aktivera]**. Tryck på **F10**.
16. Använd vänster eller höger piltangent för att gå till **Arkiv**. Använd upp- eller ned-piltangenterna för att gå till **Save Changes and Exit [Spara ändringarna och Avsluta]**. Tryck på **Retur**, och därefter på **F10** för att bekräfta.
17. Gör så här när Windows har öppnats:

    Om du använder Windows XP Professional eller Home Edition klickar du på **Start > All Programs [Starta alla program] > HP ProtectTools Inbyggda säkerhetsverktyg > Initieringsguide för den inbyggda säkerhetsanordningen**.

    Om du använder Windows 2000 klickar du på **Start > Programs [Starta program] > HP ProtectTools inbyggda säkerhetsverktyg > Initieringsguide för den inbyggda säkerhetsanordningen**.
18. Klicka på **Nästa**.
19. Skriv ett Take Ownership-lösenord och bekräfta det. Klicka på **Nästa**.

Skriv noga; av säkerhetsskäl visas inte tecknen som du skriver på skärmen.

---

20. Kontrollera att Create a new recovery archive [Skapa ett nytt återställningsarkiv] har markerats. Under **Recovery archive location [Plats för Återställningsarkivet]** klickar du på **Bläddra**.
21. Godkänd inte standardfilnamnet. Skriv ett nytt filnamn så att inte det ursprungliga filnamnet skrivs över.
22. Klicka på **Spara** och därefter på **Nästa**.
23. Skriv ett Emergency Recovery-lösenord, bekräfta detta och klicka sedan på **Nästa**.
24. Sätt i en diskett som du kan spara Nyckeln till Nödåterställningstecken på. Klicka på **Bläddra** och markera disketten.
25. Godkänd inte standardnyckelnamnet. Skriv ett nytt nyckelnamn så att inte den ursprungliga nyckeln skrivs över.

26. Klicka på **Spara** och därefter på **Nästa**.
27. Klicka på **Nästa** för att bekräfta inställningarna innan säkerhetssystemet har initierats.

Eventuellt visas ett meddelande om att Basic User-nyckeln inte kan laddas. Klicka inte i meddelandet; detta ska användas senare i proceduren och meddelandet försvinner efter någon sekund.

28. Klicka på **Nästa** för att komma förbi konfigurering av lokala bestämmelser.
29. Klicka i och rensa kryssrutan **Start Embedded Security User Initialization Wizard [Start av initieringsguide för den inbyggda säkerhetsanordningen]**. Klicka på **Slutför**.
30. Högerklicka på ProtectTools-ikonen iverktygsfältet och klicka på **Initialize Embedded Security restoration [Initiera återställning av den inbyggda säkerhetsanordningen]**.

    Detta kommando startar HP ProtectTools Embedded Security Initialization Wizard [Initieringsguiden för HP ProtectTolls inbyggda säkerhetsanordning].
31. Klicka på **Nästa**.
32. Sätt i disketten med den sparade, ursprungliga Nyckeln för nödåterställningstecken. Klicka på **Bläddra**, och leta upp återställningstecknet. Dubbelklicka på detta så att dess namn anges i fältet. Standardplatsen A:\SPEmRecToken.xml.
33. Skriv det ursprungliga Token-lösenordet och klicka på **Nästa**.
34. Klicka på **Bläddra**, och leta upp det ursprungliga återställningsarkivet. Dubbelklicka på detta så att namnet anges i fältet. Standardplatsen är C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Klicka på **Nästa**.
36. Klicka på datorn som ska återställas och därefter på **Nästa**.
37. Klicka på **Nästa** för att godkänna inställningarna.

38. Om guiden anger att säkerhetssystemet har återställts, går du till steg 39.

    Om guiden anger att återställningen misslyckades, går du tillbaka till steg 10. Kontrollera lösenord, tecknets plats och namn, arkivets plats och namn noga.

39. Klicka på Slutför.

40. Om du använder Windows XP Professional eller Home Edition klickar du på **Start > All Programs [Starta alla program] > HP ProtectTools inbyggda säkerhetsverktyg > Användarinitieringsguiden**.

    Om du använder Windows 2000 klickar du på **Start > Programs [Starta program] > HP ProtectTools inbyggda säkerhetsverktyg > Användarinitieringsguiden**.

41. Klicka på **Nästa**.

42. Klicka på **Recover your basic user key [Återställ din huvudanvändarnyckel]** och klicka på **Nästa**.

43. Välj en användare, skriv det ursprungliga Huvudanvändarnyckel-lösenordet för denna användare och klicka sedan på **Nästa**.

44. Klicka på **Nästa** för att godkänna inställningarna och standardplatsen för återställningsdata.

Steg 45 för att 49 återskapa den ursprungliga Basic User-konfigurationen.

45. Välj lämpliga säkerhetsfunktioner och klicka på **Nästa**.

46. Markera lämplig e-postklient genom att klicka på den och därefter på **Nästa**.

47. Klicka på Encryption Certificate [Kryptocertifikat] och därefter på **Nästa** för att tillämpa det.

48. Klicka på **Nästa** för att godkänna inställningarna.

49. Klicka på **Slutför**.

50. Starta om datorn.

SE UPP! Skydda Basic User-lösenordet. **Krypterad data är inte åtkomlig och kan inte heller återställas utan detta lösenord**.

DriveLock

DriveLock är en säkerhetsfunktion som förhindrar obehörig åtkomst till data på MultiBay-hårddiskar. DriveLock har installerats som en utökning av setup-programmet. Den är endast tillgänglig när DriveLock-kapabla hårddiskar upptäcks.

DriveLock är till för HP-kunder där datasäkerheten är av största betydelse. För sådana kunder är kostnader för hårddisk eller förlust av data på den ointressanta, jämfört med skada som kan orsakas av obehörig åtkomst till hårddiskens innehåll. För att kunna ha denna säkerhetsnivå och fortfarande kunna komma åt data om ett lösenord glöms bort, använder HP två lösenord för DriveLock. Ett lösenord är avsett att ställas in och definieras av systemadministratören och det andra lösenordet ställs in och används av användaren. Det finns ingen utväg för att låsa upp enheten om båda lösenorden glöms bort. När DriveLock används är det därför säkrast att data på enheten också kopieras till företagets informationsystem eller regelbundna säkerhetskopior görs.

Om båda lösenorden till DriveLock skulle glömmas bort blir hårddisken oanvändbar. För användare som inte passar in i denna kundprofil kan detta vara en oacceptabelt hög risk. För användare som passar in i denna kundprofil kan det vara en rimlig risk att ta, för att skydda innehållet på hårddisken.

Använda DriveLock

Alternativet DriveLock visas under Security (Säkerhet) i setup-programmet. Användaren kan ställa in huvudlösenordet eller aktivera DriveLock. Ett användarlösenord måste ges för att kunna aktivera DriveLock. Eftersom den ursprungliga konfigureringen av DriveLock normalt görs av en systemadministratör, måste först ett huvudlösenord ställas in. HP rekommenderar att systemadministratörer ställer in ett huvudlösenord oavsett om DriveLock ska aktiveras eller inte. Detta ger administratören möjlighet att ändra DriveLock-inställningarna om hårddisken senare är låst. När huvudlösenordet väl ställts in kan systemadministratören aktivera DriveLock eller ha den avstängd.

Om det finns en låst hårddisk, kommer POST att kräva lösenord för att låsa upp den. Om ett startlösenord har ställts in och är samma som användarlösenordet, behöver du bara ange lösenordet en gång. Om de är olika måste du även ange ett lösenord för DriveLock. Antingen huvud- eller användarlösenordet kan användas. Användaren har två försök att ange rätt lösenord. Om det misslyckas båda gångerna kommer POST att fortsätta, men data på hårddisken kommer att förbli oåtkomliga.

DriveLock-tillämpningar

Den mest praktiska användningen av DriveLock-funktionen är i en företagsmiljö där en systemadministratör förser vissa användares datorer med MultiBay-hårddiskar. Systemadministratören kan ansvara för konfigurering av MultiBay-hårddiskarna, vilket bl.a. innefattar inställning av huvudlösenord för DriveLock. Om en användare glömmer sitt användarlösenord eller om utrustningen ska användas av en annan anställd, kan huvudlösenordet användas för att ändra användarlösenordet så att hårddisken blir åtkomlig.

HP rekommenderar att företagets systemadministratörer som vill aktivera DriveLock, också sätter upp regler för hur huvudlösenord ska ställas in och underhållas. Detta för att inte en anställd ska kunna ställa in båda DriveLock-lösenorden och sedan sluta på företaget. I detta fall skulle hårddisken bli oanvändbar och behöva bytas ut. Genom att inte ställa in ett huvudlösenord kan systemadministratören å andra sidan bli utelåst från hårddisken och oförmögen att göra rutinkontroller av otillåten programvara och annan inventariekontroll samt att utföra support.

För användare med lägre säkerhetskrav rekommenderar HP att DriveLock inte aktiveras Användare i denna kategori är de som inte vanligtvis har känslig information på sin hårddisk. För dessa är risken att förlora en hårddisk genom att glömma lösenorden mycket allvarligare än den skada som kan uppstå till följd av otillåten hårddiskåtkomst. Tillgång till setup-programmet och DriveLock kan begränsas med setup-lösenordet. Genom att ange ett Setup-lösenord som inte ges till användarna, kan systemadministratören hindra användarna från att aktivera DriveLock.

SmartCover-sensor

SmartCover-sensor finns på en del modeller och är en kombination av maskin- och programvara som kan varna när datorns lock eller sidoplåt har tagits bort. Det finns tre skyddsnivåer som beskrivs i tabellen nedan.

SmartCover-sensorns skyddsnivåer

Nivå	Inställning	Beskrivning
Nivå 0	Avaktiverad	SmartCover-sensor är avaktiverad (standardinställning).
Nivå 1	Varna användaren	När datorn startas om visas ett meddelande om datorns lock eller sidoplåt har tagits bort.
Nivå 2	Lösenord för Setup-programmet	När datorn startas om visas ett meddelande om datorns lock eller sidoplåt har tagits bort. Du måste ange setup-lösenordet för att kunna fortsätta.

✎ Dessa inställningar kan ändras med setup-programmet. Mer information om setup-programmet finns i *Konfigureringshandboken*.

Ange skyddsnivå för SmartCover-sensorn

Ange en skyddsnivå för SmartCover-sensorn på följande sätt:

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start > Avsluta > Starta om datorn**.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.

✎ Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. Välj **Säkerhet** och sedan **Smart Cover** och följ anvisningarna på skärmen.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna** och **Avsluta**.

SmartCoverLock

SmartCoverLock är ett programkontrollerat lås för lock/sidoplåt som finns i vissa HP-datorer. Låset gör att obehöriga inte kan komma åt interna komponenter. Datorn levereras med SmartCoverLock i olåst läge.

SE UPP! För maximal säkerhet mot öppning av locket, ställer du in ett setup-lösenord. Setup-lösenordet hindrar obehörig åtkomst till setup-programmet.

SmartCoverLock finns som tillval för vissa system.

Låsa med SmartCoverLock

Om du vill aktivera och låsa med SmartCoverLock gör du på följande sätt:

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start >Avsluta > Starta om datorn**.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. Välj **Säkerhet** sedan **Smart Cover** och sedan **Låst**.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna** och **Avsluta**.

Låsa upp SmartCoverLock

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start >Avsluta > Starta om datorn**.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. Välj **Säkerhet > Smart Cover > Olåst**.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna** och **Avsluta**.

Använda SmartCover FailSafe Key

Om du aktiverar SmartCoverLock och inte kan ange lösenordet för att avaktivera låset måste du använda SmartCover FailSafe Key för att öppna datorn. Verktyget behövs då följande inträffar:

- Strömavbrott
- Misslyckad start
- Datorkomponentfel (t ex processor eller nätaggregat)
- Bortglömt lösenord

SE UPP! SmartCover FailSafe Key är ett specialverktyg som kan rekvireras från HP. Planera i förväg och beställ en FailSafe Key från en auktoriserad återförsäljare eller servicegivare innan du behöver den.

Du kan erhålla FailSafe Key på något av följande sätt:

- Kontakta en auktoriserad HP-återförsäljare eller servicegivare.
- Ring lämpligt nummer som finns angivet i garantin.

Mer information om hur SmartCover FailSafe Key används finns i din *Referenshandbok.*

Master Boot Record Security (MBR-säkerhet)

MBR (Master Boot Record) innehåller den information som behövs för att en hårddisk ska kunna starta upp och att dess data blir åtkomlig. MBR-säkerhet kan hindra oavsiktliga eller uppsåtliga ändringar av MBR, exempelvis sådana som orsakas av vissa datorvirus eller oriktig användning av vissa hårddiskprogram. Det hjälper dig också att återställa den senast kända fungerande MBR om förändringar av MBR upptäcks när systemet startas om.

För att aktivera MBR-skyddet gör du så här:

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start > Avsluta > Starta om datorn**.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. Välj **Säkerhet > Master Boot Record-säkerhet > Aktiverad**.
4. Välj **Säkerhet > Spara Master Boot Record**.
5. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna** och **Avsluta**.

När MBR-skyddet är aktiverat hindrar BIOS alla ändringar av MBR på aktuell startdisk under MS-DOS eller Felsäkert läge i Windows.

De flesta operativsystem sköter åtkomsten till MBR på aktuell startdisk. BIOS kan inte förhindra ändringar som görs medan operativsystemet körs.

Varje gång datorn startas eller startas om jämför BIOS MBR på aktuell startdisk med den MBR som tidigare sparats. Följande meddelande visas om förändringar upptäcks och om aktuell startdisk är samma som den sparade MBR kommer ifrån:

1999 – Master Boot Record har ändrats.

Tryck på valfri tangent för att öppna Inställningar för att konfigurera MBR-säkerhet.

När du startar setup-programmet måste du

- Spara MBR från aktuell startdisk,
- Återställa tidigare sparad MBR, eller
- Avaktivera MBR-skyddet.

Du måste känna till eventuellt lösenord.

Följande meddelande visas om förändringar upptäcks och om aktuell startdisk **inte** är samma som den sparade MBR kommer ifrån:

2000 – Master Boot Record-hårddisken har ändrats.

Tryck på valfri tangent för att öppna Inställningar för att konfigurera MBR-säkerhet.

När du startar setup-programmet måste du

- Spara MBR från aktuell startdisk, eller
- Avaktivera MBR-skyddet.

Du måste känna till eventuellt lösenord.

Om den tidigare sparade MBR mot förmodan blivit felaktig, visas följande meddelande:

1998 – Master Boot Record har förlorats.

Tryck på valfri tangent för att öppna Inställningar för att konfigurera MBR-säkerhet.

När du startar setup-programmet måste du

- Spara MBR från aktuell startdisk, eller
- Avaktivera MBR-skyddet.

Du måste känna till eventuellt lösenord.

Innan du partitionerar eller formaterar aktuell startdisk

Kontrollera att MBR-skyddet är avaktiverat, innan du ändrar partitionering eller formatering på aktuell startdisk. Många hårddiskprogram (exempelvis FDISK och FORMAT) försöker uppdatera MBR. Om MBR-skyddet är aktivt när du ändrar partitionering eller formatering på disken, kan du få felmeddelanden från hårddiskprogrammet eller en varning från MBR-skyddsfunktionen nästa gång datorn startas eller startas om. För att avaktivera MBR-skyddet gör du så här:

1. Starta eller starta om datorn. Om du är i Windows, klickar du på **Start > Avsluta > Starta om datorn**.
2. Tryck på tangenten **F10** så snart den gröna lampan på skärmen lyser. Vid behov kan du trycka på **Retur** för att komma förbi huvudskärmen.

Om du inte trycker på tangenten **F10** vid rätt tillfälle, måste du stänga av datorn, sedan starta om den och trycka på tangenten **F10** igen för att öppna programmet.

3. Välj **Säkerhet > Master Boot Record-säkerhet > Avaktiverad**.
4. Innan du avslutar, sparar du ändringarna genom att klicka på **Arkiv > Spara ändringarna** och **Avsluta**.

Kabellåsfäste

På datorns baksida finns ett kabellås så att datorn kan låsas fast vid arbetsplatsen.

Anvisningar med bilder finns i *Referenshandboken* på cd-skivan *Documentation Library.*

Identifikation med fingeravtryck

Med HPs fingeravtrycksidentifiering behöver du inget lösenord, nätverkssäkerheten förbättras, inloggningsprocessen förenklas och kostnaderna för nätverkshanteringen i företaget minskar. Nu kostar det inte längre så mycket att det bara passar HiTech-företag med höga säkerhetskrav.

Stöd för fingeravtrycksidentifikation finns i vissa modeller.

Mer information finns på:

http://h18000.www1.hp.com/solutions/security.

Felvarningar och återställning

Funktionerna för felvarningar och återställning kombinerar maskin- och programvara så att förlust av viktig information förhindras och antalet oavsiktliga stillestånd minimeras.

När ett fel inträffar, visas ett lokalt varningsmeddelande med information om felet och rekommenderade åtgärder. Du kan då visa aktuell systemstatus med hjälp av HP Client Manager. Om datorn är ansluten till ett nätverk som hanteras av HP Insight Manager, HP Client Manager eller andra systemhanteringsprogram skickar datorn också en varning om felet till nätverkshanteraren.

DPS (Drive Protection System)

DPS (Drive Protection System) är ett diagnostiskt verktyg som är förinstallerat på hårddisken i vissa HP-datorer. DPS är avsedd för att underlätta dignos av problem, som kan leda till att du slipper onödiga byten av hårddiskar.

När HP-datorer byggs testas varje hårddisk med DPS och en permanent post med nyckelinformation skrivs till hårddisken. Varje gång DPS körs skrivs testresultatet till hårddisken. Servicegivaren kan använda informationen för att diagnostisera de förhållanden som ledde till att DPS-programmet kördes. Instruktioner för användning av DPS finns i *Felsökningshandboken*.

Nätaggregat med överspänningsskydd

Ett nätaggregat med inbyggt överspänningsskydd ger ökat skydd om datorn utsätts för snabba överspänningar. Nätaggregatet kan klara spänningstoppar på upp till 2 000 V utan systemavbrott eller dataförluster.

Termisk sensor

Den termiska sensorn är en kombinerad maskin- och programvarufunktion som övervakar datorns inre temperatur. Funktionen visar ett varningsmeddelande vid temperaturväxlingar utanför det normala temperaturintervallet, så att du kan åtgärda felet innan interna komponenter skadas eller data förloras.

Index

L

M

N

O

P

R

S

T

U

V

W